**Cyber-Influence Operation Analysis:**

**Background, Documentation, and Modelling of Cyber and Disinformation Components.**

# GRU 2022 Campaign: “Ukraine-Russia DDoS attack on Ukrainian Banks and other government services”.

## Summary

Ukrainian banks and other government services were subject to a DDoS attack as part of the current Ukraine-Russia conflict. Prior to the physical war starting, cyber-warfare was a prevalent tool used by either party. The cyber-information operation in question is a reflection DDoS attack on two of Ukraine’s largest banks. The attack occurred on Tuesday 15th of February 2022 and targeted many websites including Privatbank and Oschadbank. The attack was successful in rendering some services offline.

## Timeline and Context

The Russian-Ukrainian conflict has been long standing. Tensions have steadily increased, with malicious activity often occurring before the kinetic warfare began.

The attack occurred on Tuesday 15th of February 2022 and targeted many websites including Privatbank and Oschadbank. The attack was successful in rendering some services offline.1,2.

* As Russian forces gathered along the border, many Ukrainians were unable access the online services of the banks.
  + The adversary carried out the DDoS by using the CLDAP searchRequest operation – carrying out reflection attacks.
* Following the attack, customers of the bank were the target of fake messages.
  + PrivatBank customers received texts while Oschadbank customers were targeted via social media. The U.S. White House attributed the cyber-attack to Russia’s largest foreign-intelligence agency, the GRU.
  + Messages claiming the bank doesn’t work and their services are down aim to drive more traffic to the bank websites, adding to the DDoS incident, and increase fear and uncertainty regarding the Ukrainian government’s ability to protect itself.

## Frameworks

### ATT&CK Framework

* **TA0040: Impact**
  + **T1499.002:** Endpoint Denial of Service: Service Exhaustion Flood
    - Adversaries may target the different network services provided by systems to conduct a denial of service (DoS).
    - *The adversary carried out a DDoS attack on the bank’s network.*

### DISARM Framework

* **PLAN:**
  + **TA01: Plan Strategy**
    - **T0073**: Determine Target Audience
    - **T0074**: Determine Strategic Ends
  + **TA02: Plan Objectives**
    - **T0066**: Degrade Adversary
  + **TA13: Target Audience Analysis**
    - **T0072**: Segment Audiences
      * **T0072.002**: Demographic Segmentation
* **PREPARE:**
  + **TA14: Develop Narratives**
    - **T0082**: Develop New Narratives
    - **T0022.002**: Develop Original Conspiracy Theory Narratives
  + **TA06: Develop Content**
    - **T0085**: Develop Text-based Content
      * **T0085.001**: Develop AI-Generated Text
      * **T0085.003** Develop Inauthentic News Articles
    - **T0086**: Develop Image-based Content
      * **T0086.001**: Develop Memes
      * **T0086.002**: Develop AI-Generated Images
    - **T0087**: Develop Video-based Content
      * **T0087.001**: Develop AI-Generated Videos
  + **TA15: Establish Social Assets**
    - **T0007**: Create Inauthentic Social Media Pages and Groups
    - **T0013**: Create inauthentic websites
    - **T0090**: Create Inauthentic Accounts
      * **T0090.001**: Create Anonymous Accounts
      * **T0090.002**: Create Cyborg
      * **T0090.003**: Create Bot Accounts
    - **T0093**: Acquire/Recruit Network
      * **T0093.002**: Acquire Botnets
      * **T0093.004**: Infiltrate Existing Networks
  + **TA16: Establish Legitimacy**
    - **T0009**: Create fake experts
    - **T0011**: Compromise legitimate accounts
    - **T0098**: Establish Inauthentic News Sites
      * **T0098.001**: Create Inauthentic News Sites
      * **T0098.002**: Leverage Existing Inauthentic News Sites
    - **T0100**: Co-opt Trusted Sources
      * **T0100.001**: Co-opt Trusted Individuals
      * **T0100.003**: Co-opt Influencers
  + **TA05: Micro target**
    - **T0016**: Create Clickbait
  + **TA07: Select Channels and Affordance**
    - **T0104**: Social Networks
      * **T0104.001**: Mainstream Social Networks
      * **T0104.002**: Dating Apps
      * **T0104.003**: Private/Closed Social Networks
      * **T0104.004**: Interest-Based Networks
      * **T0104.005**: Use hashtags
      * **T0104.006**: Create dedicated hashtag
    - **T0105**: Media Sharing Networks (e.g., TikTok, Instagram)
    - **T0106**: Discussion Forum (e.g., Reddit)
    - **T0111**: Traditional Media
      * **T0111.002**: Newspaper
* **EXECUTE:**
  + **TA09: Deliver Content**
    - **T0115**: Post Content
      * **T0115.001**: Share Memes
      * **T0115.003**: One-Way Direct Posting
  + **TA17: Maximise Exposure**
    - **T0049**: Flooding the information space (and sub techniques)
    - **T0119**: Cross-Posting (and sub techniques)
    - **T0121**: Manipulate Platform Algorithm
  + **TA18: Drive Online Harms**
    - **T0123**: Control Information Environment through Offensive Cyberspace Operations
      * **T0123.001**: Delete Opposing Content
    - **T0124**: Suppress Opposition
      * **T0124.001**: Report Non-Violate Opposing Content
  + **TA10: Drive Offline Activity**
    - **T0057**: Organise Events (e.g., Protests)
  + **TA11: Persist in the Information Environment**
    - **T0060**: Continue to Amplify
* **ASSESS:**
  + **TA12: Assess Effectiveness**
    - **T0133**: Measure Effectiveness
      * **T0133.001**: Behavior changes
      * **T0133.005**: Action/attitude
    - **T0134**: Measure Effectiveness Indicators (or KPIs)
      * **T0134.001**: Message reach
      * **T0134.002**: Social media engagement

## Resources

Ji, J. (2022) *Reflective and short-burst ddos attacks harnessed to knock down the targets in Ukraine*, *NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks*. Available at: <https://nsfocusglobal.com/reflective-and-short-burst-ddos-attacks-harnessed-to-knock-down-the-targets-in-ukraine/>.

Tsvetkova , M. et al. (2022) *Ukraine Defence Ministry website, Banks, knocked offline | reuters*. Available at: <https://www.reuters.com/world/europe/ukraine-reports-cyber-attack-defence-ministry-website-banks-tass-2022-02-15/>.

Uchill, J. (2022) *Officials: Russia likely cause of cyberattacks on Ukraine, but ‘no specific credible threats to the US homeland’*, *SC Media. Risk Assessments/Management, Threat Intelligence*. Available at: <https://www.scmagazine.com/analysis/officials-russia-likely-cause-of-cyberattacks-on-ukraine-but-no-specific-credible-threats-to-the-us-homeland>.

Masters, J. (2022) *Russia-Ukraine war: Cyberattack and kinetic warfare timeline*, *MSSP Alert*. Available at: <https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion>.